МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «ЛИЦЕЙ» Р.П. СТЕПНОЕ СОВЕТСКОГО РАЙОНА САРАТОВСКОЙ ОБЛАСТИ

Рассмотрено и рекомендовано на
заседании педагогического совета
Протокол № 1
от 30 августа 2023г.

«УТВЕРЖДЕНО»
Директор МБОУ «Лицей» р.п. Степное
Советского района Саратовской области
Приказ от 30 августа 2023г. № 159

Миткевич Елена Юрьевна
Подписано цифровой подписью: Миткевич Елена Юрьевна
Дата: 2023.08.30 08:14:01 +03'00'

ДОПОЛНИТЕЛЬНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ (ОБЩЕРАЗВИВАЮЩАЯ) ПРОГРАММА

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Направленность: техническая

Срок реализации: 9 месяцев

Возраст детей: 15-17 лет

Составитель программы:

Голубева Татьяна Ивановна

педагог дополнительного образования

р.п. Степное, 2023г.

1. Комплекс основных характеристик программы

1.1. Пояснительная записка

Рабочая программа курса дополнительного образования «Информационная безопасность» составлена на основе Положения о дополнительной общеобразовательной (общеразвивающей) программе МБОУ «Лицей» р. п. Степное Советского района Саратовской области

Аннотация к программе. Программа «Информационная безопасность» имеет высокую актуальность и отражает важные вопросы безопасной работы с новыми формами коммуникаций и услуг цифрового мира: потребность в защите персональной информации, угрозы, распространяемые глобальными средствами коммуникаций Интернет и мобильной связи, использующими рассылки сообщений, электронную почту, информационно-коммуникативные ресурсы взаимодействия в сети Интернет через массово доступные услуги электронной коммерции, социальные сервисы, сетевые объединения и сообщества, ресурсы для досуга (компьютерные игры, видео и цифровое телевидение, цифровые средства массовой информации и новостные сервисы), а также повсеместное встраивание дистанционных ресурсов и технологий в учебную деятельность, использующую поиск познавательной и учебной информации, общение в социальных сетях, получение и передачу файлов, размещение личной информации в коллективных сервисах. Помимо профилактики информационных угроз и противоправных действий через ресурсы в сети Интернет и мобильные сети, крайне актуально использовать коммуникации для привлечения обучающихся к информационно-учебной и познавательно-творческой активности по использованию позитивных интернет-ресурсов: учебных, культурных, научно-популярных, интеллектуальных, читательских, медийных, правовых, познавательных ресурсов и специализированных социальных сообществ и сервисов для детских объединений и творческих мероприятий для детей и молодежи.

Отличительной особенностью является включение в контекст не только обучения, но и воспитания в условиях быстро нарастающих новых видов информационных угроз и развития средств противодействия им, отраженных в законодательстве Российской Федерации за счет оборудования «Точки роста». Программа поддерживается электронными ресурсами на основе документальных фильмов, анимационных ресурсов и электронных практикумов в открытом доступе от IT-компаний Российской Федерации в рамках их участия в проектах по информационной безопасности для детей.

Адресат программы: 15-17 лет.

Возрастные особенности. Программа ориентирована на подростков 15-17 лет, проявляющих желание углубить и расширить свои знания правовой культуры информационной безопасности при работе в сети Интернет. Программа реализуется с учетом психологических возможностей этого возрастного периода, сочетая принцип группового обучения с индивидуальнымподходом и интенсивной продуктивной формой занятий.

Предусмотрены следующие формы организации образовательного процесса - групповые, фронтальные виды занятий: выполнение диагностических тестов и опросов, исследовательских и самостоятельных работ. Учащиеся данного возраста способны на высоком уровне усваивать разнообразную информацию.

Программа реализуется на русском языке, с использованием модуля дистанционного (сетевого) обучения.

Объем: 36 часов.

Срок освоения программы: 9 месяцев.

Режим занятий: 1 занятие в неделю по 45 минут.

Цель программы: обеспечить социальные аспекты информационной безопасности в воспитании культуры информационной безопасности у учащихся в условиях цифрового мира, включение на регулярной основе цифровой гигиены в контекст воспитания и обучения, формирование у выпускника лицея правовой грамотности по вопросам информационной безопасности, которые влияют на социализацию подростков в информационном обществе, формирование личностных и метапредметных результатов воспитания и обучения учащихся.

Задачи программы:

– сформировать понимание сущности и воспитывать необходимость принятия учащимися таких ценностей, как ценность человеческой жизни, свободы, равноправия и достоинства людей, здоровья, опыта гуманных, уважительных отношений с окружающими;

– создавать педагогические условия для формирования правовой и информационной культуры учащихся, развития у них критического отношения к информации, ответственности за поведение в сети Интернет и последствия деструктивных действий, формирования мотивации к познавательной, а не игровой деятельности, воспитания отказа от пустого времяпрепровождения в социальных сетях, осознания ценности живого человеческого общения;

– научить осознавать важность проектирования своей жизни и будущего своей страны - России в условиях развития цифрового мира, ценность ИКТ для достижения высоких требований к обучению профессиям будущего в мире, принимать средства в Интернете как среду созидания, а не разрушения человека и общества.

Планируемые результаты:

– сформировать у учащихся с учетом возрастных особенностей личностные результаты, которые позволят им грамотно ориентироваться в информационном мире с учетом имеющихся в нем угроз;

– сформировать коммуникативную компетентность в общении и сотрудничестве со сверстниками, детьми старшего и младшего возраста, взрослыми в процессе образовательной, общественно полезной, учебно-исследовательской, творческой и других видов деятельности;

– освоить приемы работы с социально значимой информацией, ее

осмысление; развитьспособность, учащихся делать необходимые выводы и давать обоснованные оценки социальным событиям и процессам.

К концу обучения учащиеся должны:

Знать:

– источники информационных угроз, вредоносные программы и нежелательные рассылки, поступающие на мобильный телефон, планшет, компьютер;

– роль близких людей, семьи, правоохранительных органов для устранения проблем и угроз в сети Интернет и мобильной телефонной связи, телефоны экстренных служб;

– виды информационных угроз, правила поведения для защиты от угроз, виды правовой ответственности за проступки и преступления в сфере информационной безопасности;

– проблемные ситуации и опасности в сетевом взаимодействии и правила поведения в проблемных ситуациях, ситуациях профилактики и предотвращения опасности;

– этикет сетевого взаимодействия, правовые нормы и законодательство в сфере информационной безопасности;

– правила защиты персональных данных;

– назначение различных позитивных ресурсов в сети Интернет для образования и в профессиях будущего.

Уметь:

– применять правила цифровой гигиены для использования средств защиты персональных данных (формировать и использовать пароль, использовать код защиты персонального устройства, регистрироваться на сайтах без распространения личных данных);

– применять информационно-коммуникативные компетенции по соблюдению этических и правовых норм взаимодействия в социальной сети или в мессенджере, уметь правильно вести себя в проблемной ситуации (оскорбления, угрозы, предложения, агрессия, вымогательство, ложная информация и др.), отключаться от нежелательных контактов, действовать согласно правовым нормам в сфере информационной безопасности (защиты информации).

1.2. Содержание программ

1.2.1. Учебный план

№ п/п	Тема	Количество часов			Форма контроля (аттестация)
		Теория	Практика	Всего	
Раздел 1. Информационное общество и информационная культура (24 ч.)					
1.	1.1. Понятия юридической ответственности за	2	0	2	Входной контроль. Беседа

	правонарушения в области информационной безопасности.				
2.	1.2. Нормативное обеспечение информационной безопасности в Российской Федерации.	2	0	2	Текущий контроль. Опрос
3.	1.3. Законодательство Российской Федерации о гражданско-правовой ответственности. Понятие гражданско-правовой ответственности.	1	1	2	Текущий контроль. Тестирование
4.	1.4. Гражданско-правовая ответственность несовершеннолетних за проступки в области информационной безопасности (защиты информации).	2	1	3	Текущий контроль. Тестирование
5.	1.5. Законодательство Российской Федерации об административной ответственности в сфере информационной безопасности. Понятие административной ответственности.	2	2	4	Текущий контроль. Опрос
6.	1.6. Административная ответственность несовершеннолетних граждан за проступки в области информационной безопасности (защиты информации).	3	2	5	Текущий контроль. Тестирование
7.	1.7. Законодательство Российской Федерации об уголовной ответственности в сфере информационной	1	0	1	Текущий контроль. Опрос

	безопасности. Понятие уголовной ответственности.				
8.	1.8. Уголовная ответственность несовершеннолетних за преступления в области информационной безопасности (защиты информации).	2	3	5	Текущий контроль. Тестирование
Раздел 2.Информационное пространство и правила информационной безопасности (12 ч.)					
9.	2.1. Проектная работа. Нормативные основы лицензионных соглашений.	1	1	2	Текущий контроль. Опрос. Онлайн-тренажер
10.	2.2. Проектная работа. Практика соблюдения норм информационной безопасности в личном информационном пространстве.	1	2	3	Текущий контроль. Опрос. Онлайн-тренажер
11.	2.3. Практика электронного обучения и культура информационной безопасности при самостоятельной работе с коммуникациями, сервисами и ресурсами сети Интернет.	0	3	3	Текущий контроль. Опрос. Онлайн-тренажер
12.	2.4. Электронное обучение по информационной безопасности.	0	4	4	Защита проектов, исследовательских работ, докладов.
	Итого	**17**	**19**	**36**	

1.2.2. Содержание программы

Раздел 1. Информационное общество и информационная культура – 24 часа

Тема 1.1. Понятия юридической ответственности за правонарушения в области информационной безопасности – 2 часа.

Теория: Ознакомление с Программой. Ознакомление с основными понятиями, используемыми в ФЗ о защите детей от информации, причиняющей вред здоровью и развитию.

Тема 1.2. Нормативное обеспечение информационной безопасности в Российской Федерации– 2 часа.

Теория: Краткий обзор статей закона.

Тема 1.3. Понятие гражданско-правовой ответственности. Законодательство Российской Федерации о гражданско-правовой ответственности в сфере информационной безопасности – 2 часа.

Теория: Ознакомление с основными понятиями, краткий обзор статей закона.

Практическая работа: Тестирование.

Тема 1.4. Гражданско-правовая ответственность несовершеннолетних за проступки в области информационной безопасности (защиты информации) – 3 часа.

Теория: Ознакомление с основными понятиями, краткий обзор статей закона.

Практическая работа: Тестирование.

Тема 1.5. Понятие административной ответственности. Законодательство Российской Федерации об административной ответственности в сфере информационной безопасности – 1 час.

Теория: Ознакомление с основными понятиями, краткий обзор статей закона.

Тема 1.6. Административная ответственность несовершеннолетних граждан за проступки в области информационной безопасности (защиты информации) – 6 часов.

Теория: Ознакомление с основными понятиями, краткий обзор статей закона.

Практическая работа: Тестирование.

Тема 1.7. Понятие уголовной ответственности. Законодательство Российской Федерации об уголовной ответственности в сфере информационной безопасности – 1 час.

Теория: Ознакомление с основными понятиями, краткий обзор статей закона.

Тема 1.8. Уголовная ответственность несовершеннолетних за преступления в области информационной безопасности (защиты информации) – 5 часов.

Теория: Ознакомление с основными понятиями, краткий обзор статей закона.

Практическая работа: Тестирование.

Раздел 2. Информационное пространство и правила информационной безопасности – 12 часов

Тема 2.1. Проектная работа. Нормативные основы лицензионных соглашений – 2 часа.

Теория:Ознакомление с нормативными основами лицензионных соглашений.

Практическая работа:в онлайн-тренажере пройти набор потенциально опасных ситуаций, с использованием ИКТ «Безопасность в Интернет» (https://xn--h1adlhdnlo2c.xn--p1ai/lessons/bezopasnost-v-internete-2018-2019).

Тема 2.2. Проектная работа. Практика соблюдения норм информационной безопасности в личном информационном пространстве – 3 часа.

Теория:Ознакомление с основнымипонятиями и нормами.

Практическая работа: онлайн-тренажер «Безопасность будущего» (https://xn--h1adlhdnlo2c.xn--p1ai/lessons/bezopasnost-budushhego).

Тема 2.3. Практика электронного обучения и культура информационной безопасности при самостоятельной работе с коммуникациями, сервисами и ресурсами сети Интернет – 3 часа.

Практическая работа: в онлайн-тренажере пройти набор заданий, связанных с информационной безопасностью. Каждое задание - симуляция той или иной жизненной ситуации, в которой неосторожное поведение может привести к нежелательным последствиям (https://xn--h1adlhdnlo2c.xn--p1ai/lessons/bezopasnost-budushhego).

Тема 2.4. Электронное обучение по информационной безопасности – 4 часа.

Практическая работа: Защита проектов, исследовательских работ, докладов.

Форма аттестации планируемых результатов программы:

Контроль и диагностика образовательной деятельности учащихся осуществляется по трем направлениям.

Входной контроль проводится на первом занятии в виде анкетирования для выявления общих знаний учащихся по информационной безопасности.

Текущий контроль практических навыков осуществляется регулярно на каждом занятии. Теоретические знания проверяются по вновь приобретенным знаниям.

Итоговый контроль проходит в формате защиты проектов, исследовательских работ, докладов и подразумевает:

- самооценку учащихся;
- оценку метапредметных результатов учащихся по итогам наблюдения педагога;
- для особо одаренных детей участие в конкурсах.

В конце учащиеся оцениваются по следующим критериям:

- практичность и творческий подход;
- прилежание, работоспособность, дисциплинированность;

– уровень освоения теоретического материала. В соответствии с указанными критериями выделены три уровня освоения учащимися дополнительной общеобразовательной программы: высокий, средний, ниже среднего.

Практика

Высокий уровень ставится учащемуся в том случае, если в процессе обучения и на зачетном занятии он продемонстрировал: отличные знания.

Средний уровень учащийся получает, если в процессе обучения и на зачетном занятии он продемонстрировал: частично усвоенный материал.

Уровень ниже среднего ставится учащемуся, если в процессе обучения и на зачетном занятии он продемонстрировал: не желание освоить программу.

Теория

Высокий уровень ставиться в случае выполнения тестовых заданий с уровнем правильных ответов 90-100%.

Средний уровень ставиться учащемуся, если выполнение тестовых заданий с уровнем правильных ответов 60-80%.

Уровень ниже среднего получает учащийся в том случаи, если выполнение тестовых заданий с уровнем правильных ответов 30-50%.

Итоговый контроль проводится в конце учебного года через годовой зачет, где отслеживаются уровень освоения дополнительной общеобразовательной программы, динамика усвоения теоретических и практических навыков.

Условия для реализации программы: доступность, наглядность, активность.

2. Комплекс организационно-педагогических условий

2.1. Методическое обеспечение

Методы обучения, используемые на занятиях:

– словесные методы обучения: объяснение, беседы, диалог, защита проектов и исследовательских работ;

– метод практической работы: онлайн-тренажеры, поисковые системы в сети Интернет;

– наглядные методы обучения: применение рисунков, плакатов, фотографий, таблиц, видео, слайдов, интерактивных роликов.

Распределяя материал по занятиям, учитываются основные дидактические принципы: систематичность, доступность, прочность.

Доступность - при изложении материала учитываются возрастные особенности детей, один и тот же материал по-разному преподается, в зависимости от возраста и субъективного опыта учащихся. Материал располагается от простого к сложному. При необходимости допускается повторение части материала, через некоторое время.

Наглядность – при его использовании человек получает через органы зрения в 5 раз больше информации, чем через слух, поэтому на занятиях

используются как наглядные материалы, так и обучающие программы.

Сознательность и активность - для активизации деятельности учащихся используются такие формы обучения, как занятия-исследования, практические занятия, совместные обсуждения поставленных вопросов и свободное творчество.

Формы обучения:

- коллективная деятельность, позволяющая подчинять свои личные интересы общей цели, воспитывать чувство ответственности, сопереживания за результаты работы всех учащихся;
- групповая деятельность, помогающая учащимся в реализации своих возможностей, организация взаимопомощи в группах;
- совместное творчество учащихся и педагога, способствующее развитию коммуникабельности учащихся;
- участие в конкурсах, соревнованиях.

На занятиях используются следующие педагогические технологии:

- технология развивающего обучения;
- коммуникативная технология обучения;
- здоровьесберегающая технология;
- личностно-ориентированные технологии.

2.2. Условия для реализации программы

2.2.1. Материально-техническая база: кабинет, оснащенный по всем требованиям безопасности и охраны труда; компьютер; принтер; колонки; мультимедиа проектор; экран; ноутбуки; тесты по основным темам на каждого учащегося; дисковые накопители.

2.2.2. Программно-методическое обеспечение:

- нормативная и учебная литература, справочный материал;
- наглядные материалы: плакаты, схемы.

2.2.3. Кадровое обеспечение: педагог дополнительного образования.

2.3. Список литературы

Для педагога:

1. Конституция Российской Федерации от 12.12.1993 (ред. от 01.08.2014).
2. Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (с изменениями и дополнениями).
3. Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы».
4. Яковлев В.А. Шпионские и антишпионские штучки: Техническая литература. Издательство: Наука и Техника, 2015, 320 с.

Для учащихся:

1. Бирюков А. А. Информационная безопасность защита и нападение, 2-е издание:Издательство: ДМК-Пресс., 2017, 434 с.
2. Колесниченко Денис. Анонимность и безопасность в интернете. От чайника кпользователю. Самоучитель Издательство: БХВ-Петербург, 2012, 240с.
3. Мазаник Сергей. Безопасность компьютера. Защита от сбоев, вирусов инеисправностей: издательство: ЭКСМО, 2014, 256 с.
4. Савченко Е. Кто, как и зачем следит за вами через интернет: Москва – Третий Рим, 2012, 100 с.

Интернет-источники:

1. Официальный интернет-портал правовой информации - http://www.pravo.gov.ru
2. Информационно-правовой портал ГАРАНТ.РУ – http://www.garant.ru
3. Всероссийский образовательный проект в сфере информационных технологий
УРОК ЦИФРЫ - https://xn--h1adlhdnlo2c.xn--p1ai/lessons/bezopasnost-v-internete-2018-2019, https://xn--h1adlhdnlo2c.xn--p1ai/lessons/bezopasnost-budushhegoc, https://xn--h1adlhdnlo2c.xn--p1ai/lessons/bezopasnost-budushhego.